

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A
Property to be Searched

A Black in color suspected Apple iPhone 14, listed under ATF case number 772120-21-0059, item 000078; hereinafter referred to as Device A



Device A, is currently located at the ATF Milwaukee Field Office at 1000 N. Water St, Suite 1400, Milwaukee, WI 53202.

ATTACHMENT B
Particular Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations Timothy SCOTT has committed of Title 18 United States Code Section 922 (g)(1), including but not limited to the following:
 - a. lists of firearms dealers and related identifying information;
 - b. types, amounts, and prices of firearm transactions, as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of firearms (including names, addresses, phone numbers, or any other identifying information);
 - d. any information related to SCOTT's purchase, receipt, or possession of firearms during the time he has been prohibited by federal law from possessing firearms;
 - e. any information recording SCOTT's schedule or travel to the present;
 - f. all bank records, checks, credit card bills, account information, and other financial records relevant to the sale and/or trade of narcotics and firearms;
 - g. photos, videos, IP addresses, contact information, contact lists;
 - h. text messages, social media messages and content, SMS messages, iMessage data, relating to the sale and/or trade of firearms;
 - i. electronic mail to include the content of the emails, and associated email addresses, relating to the sale and/or trade of firearms;
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have

been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Richard Connors, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device, more fully described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”) assigned to the Milwaukee Field Office since October of 2015. I have been employed as a full-time law enforcement officer for approximately seven years. I have received training at the Federal Law Enforcement Training Center in Glynco, GA. I attended the Criminal Investigator Training Program, as well as ATF’s Special Agent Training Program. I have received training in the investigation of unlawful possession of firearms, the unlawful transfer of firearms, and the unlawful dealing in firearms without a dealers’ license. Prior to becoming a Special Agent with the ATF, I received two bachelor’s degrees from Northern Illinois University in the fields of Sociology and International Relations. I have received a master’s degree from Northern Illinois University in the field of American Government.

3. I have received training in the investigation of firearm trafficking. Based on my training, experience, and participation in firearm trafficking investigations, I know and/or have observed the following:

- I have utilized informants to investigate firearm trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations distribute firearms in Wisconsin and elsewhere;
- I have also relied on informants to obtain firearms from individuals on the streets (as opposed to licensed gun dealers), via what are known as a controlled purchases;
- I have experience conducting street surveillance of individuals engaged in firearm trafficking. I have participated in the execution of numerous search warrants where firearms, ammunition, and magazines have been seized;
- I am familiar with the language utilized over the telephone to discuss firearm trafficking, and know that the language is often limited, guarded, and coded;
- I know that firearm traffickers often use electronic equipment to conduct these operations; and
- I know that firearm traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase and/or title these assets to avoid

scrutiny from law enforcement officials. I also know what firearm and drug traffickers may keep photographs of these items on electronic devices.

4. I have participated in multiple firearm and drug trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. On many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

5. The facts in this affidavit come from my personal observations, my training and experience, and from information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922(g)(1) (felon in possession of a firearm) have been committed and that evidence of those violations may be located at the location described in Attachment A.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is:

- Black in color suspected Apple iPhone 14, listed under ATF case number 772120-21-0059, item 000078; hereinafter referred to as Device A

Device A, is currently located at the ATF Milwaukee Field Office at 1000 N. Water St, Suite 1400, Milwaukee, WI 53202.

8. On April 25, 2023, a federal grand jury in the Eastern District of Wisconsin returned a sealed forty-three (43) count indictment against Timothy SCOTT and twenty-nine (29) other members and associates of the Wild 100's Street gang. Timothy SCOTT was indicted for one count of Mail Fraud Conspiracy, in violation of Title 18, United States Code, Section 1349; Mail Fraud, in violation of Title 18, United States Code, Sections 1341. A warrant for Timothy SCOTT's arrest was issued on April 26, 2023.

9. Your affiant is aware on May 10, 2023, ATF agents executed the arrest warrant on Timothy SCOTT at his residence located at 7854 N. 64th CT, Milwaukee, WI. Agents announced their presence at the threshold of the door and upon knocking on the door, the door swung open appearing to not being locked properly. Agents entered the residence for safety concerns and began to make further announcements of the arrest warrant for Tim SCOTT. Tim SCOTT eventually emerged from the upstairs of the residence and was taken into custody. Agents conducted a protective sweep of the residence and observed in plain view, a loaded handgun magazine inside of a open safe on a shelf in the closet of the master bedroom. The bedroom appeared to belong to an adult and not children. It should be noted three children were contacted in the living room of the residence, the children were not handcuffed and seated in the living room during the arrest of SCOTT.

10. During the arrest of Tim SCOTT, his live-in girlfriend and mother of the three young children called SCOTT's cell phone (Device A). The woman was identified as Brittany WEBB and advised she would return home. WEBB arrived home shortly after the phone call, WEBB advised she was not aware of any firearms in the residence and granted agents written and verbal consent to search the residence.

11. Agents began to search the residence. Located in the clothes hamper of the master bedroom was a Ruger handgun, model 57, 57 caliber, bearing S/N 641-40951. This is the same bedroom where several rounds of ammunition were located. Your affiant is aware this firearm was not manufactured in the state of Wisconsin and thus traveled in interstate commerce. Additionally, located in the kitchen was Timothy SCOTT's ID card and 1.7 gross grams of suspected heroin. Lastly, located next to the master bedroom closet safe where the initial handgun magazine was located was Device A.

12. It should be noted, Timothy SCOTT is a convicted felon from state of Georgia (Cobb County Superior Court) for charge number 88422884373002 for possession of cocaine. SCOTT was convicted in this case on or about April 1, 2022. 04/01/2022. Additionally, SCOTT's most recent Wisconsin felony conviction is in State of Wisconsin court case 2018CF001306 for Possession of THC (2nd offense). SCOTT is not lawfully allowed to possess firearms or ammunition.

13. Your affiant is aware convicted felons will utilize cell phones to acquire firearms. The phones are used to set up purchases, send photos, and arrange

transactions. Your affiant believes there could be evidence of federal violations on Device A. Your affiant has worked multiple investigations involving prohibited persons utilizing cell phones to arrange the acquisition of firearm via cell phone and evidence of that action is often present on the target cell phone.

14. The Device are currently in the lawful possession of ATF. ATF seized Device A, during a consent search in connection with the arrest on a federal arrest warrant. I seek this additional warrant out of an abundance of caution to be certain that an examination of Device A, will comply with the Fourth Amendment and other applicable laws.

15. Device A is currently in storage at the ATF Milwaukee Field Office at 1000 N. Water St, Suite 1400, Milwaukee, WI 53202. Device A, is inventoried under ATF inventory number 000078, under case number 772120-21-0059. In my training and experience, I know that Device A, has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the ATF.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless

telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. *Digital camera:* A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. *Portable media player:* A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. *GPS:* A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals

are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at www.samsung.com, I know that the Device has capabilities that allow it to serve as a

wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

22. Based on all of the aforementioned information as well as my training and experience and the investigation to date, your affiant believes there is probable cause to search Timothy SCOTT's cell phones which may contain evidence of his violations of Title 18, United States Code, Section 922(g)(1) (Felon in possession of a firearm).

ATTACHMENT A
Property to be Searched

A Black in color suspected Apple iPhone 14, listed under ATF case number 772120-21-0059, item 000078; hereinafter referred to as Device A



Device A, is currently located at the ATF Milwaukee Field Office at 1000 N. Water St, Suite 1400, Milwaukee, WI 53202.

ATTACHMENT B
Particular Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations Timothy SCOTT has committed of Title 18 United States Code Section 922 (g)(1), including but not limited to the following:
 - a. lists of firearms dealers and related identifying information;
 - b. types, amounts, and prices of firearm transactions, as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of firearms (including names, addresses, phone numbers, or any other identifying information);
 - d. any information related to SCOTT's purchase, receipt, or possession of firearms during the time he has been prohibited by federal law from possessing firearms;
 - e. any information recording SCOTT's schedule or travel to the present;
 - f. all bank records, checks, credit card bills, account information, and other financial records relevant to the sale and/or trade of narcotics and firearms;
 - g. photos, videos, IP addresses, contact information, contact lists;
 - h. text messages, social media messages and content, SMS messages, iMessage data, relating to the sale and/or trade of firearms;
 - i. electronic mail to include the content of the emails, and associated email addresses, relating to the sale and/or trade of firearms;
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have

been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.